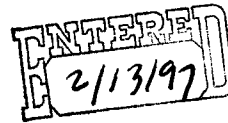# V-ONE

Security for a Connected World

February 12, 1997

Nancy Crowe
Regulatory Policy Division, Room 2705
Bureau of Export Administration, Department of Commerce
14th Street and Pennsylvania Ave., N.W.
Washington, D.C. 20230.

Dear Ms. Crowe:

V-ONE Corporation is a firm providing software and hardware tools that secure users of the Internet and Intranets. Its customers are large, international firms including banks, telephone service providers, credit card firms, financial services companies, government agencies and industrial firms of all kinds. Although the company is only four years old, it has become well known in the industry. We believe it has a major niche in the computer security business.

V-ONE has received export approval for its products in two ways. One is for specific customer applications that have the ability to qualify for a moderate level of encryption using 56 bit DES algorithms. They can obtain export licenses. The others are limited to use 40 bit RC4 based encryption under the mass market rules that do not require individual end-user licenses.

Our international clients are, in most cases, very concerned with the quality of protection afforded by the 40 bit RC4 security. Two weeks ago, a Berkeley student justified their concern when he succeeded in breaking a message protected with that level of security in only 3.5 hours. The fact that he used a large number (259) of computers to do it, isn't of interest to our clients. When they are transferring large amounts of money under the security we provide, a hacker could easily justify investing in whatever processing power is necessary to accomplish the task.

In some cases, the clients' governments have imposed a ruling that the minimum level of acceptable security is 56 bit DES. Thus, depending on their ability to obtain export licenses for DES, we may be unable to sell them our products.

Consequently, it was a welcome message when the Administration announced last November that they were relaxing export regulations. But it was unwelcome when we received the regulations themselves and we found that the complexity of administration necessary to comply with the requirements would provide little solace to either V-ONE or its customers. Subsequently, we determined that by using the "client managed key recovery option" there was hope that we could work out a solution acceptable to at least some clients. We are pursuing that method in a proposal now being submitted for approval.

The Problem:

Although many of our clients are, or would like to be, moving large valued transactions electronically, the amount they are willing to spend for security is always limited. Historically, security has been very difficult to sell at any price, mostly because customers don't think it necessary. The Internet has changed the awareness of many clients, however; and they are realizing that there is NO protection for their data without security add-ons for data moving through the Internet. Nonetheless, they are still reluctant to spend substantial money to implement security. Imposition of complex or difficult user administration to implement security is another barrier. Policies, rules, administration and other processes add more to the reluctance of the customers.

The Key Escrow proposal has been especially difficult for our customers to accept. Now, in addition to the imposition of complex rules, arrangements and policies, in order to have strong security, they are asked to rely on a "*trusted* third party" for security services. They thus have no direct control of their security and must rely on someone else to protect their interests. If they suffer a sizeable loss due to a failure of the third party to protect their data properly, they won't even have a method to prove that the exposure was due to the third party's negligence. Needless to say, they aren't pleased.

If there were no other options, it might be different. But there are other options, although not from US sources. Many international vendors of competent security software and hardware are most anxious to provide strong, uncompromised security tools. And they can do so at an attractive price. So why should customers buy our product or any other US brand?

Customer operated Key Recovery provides customers a greater control. Even US firms may justify operating with this capability, since customers may occasionally need to monitor what one of their own internal people is sending in the event of suspected fraud or questionable actions. Although the need to meet BXA requirements is stringent, efforts required to meet the BXA regulations will strengthen their security. A court order would provide access to only one of their people's data, and it will only expose one session with no permanent compromise of that user's other data.

For the Export Administration Regulation to work, foreign governments must accede to US BXA regulations. Bilateral agreements are a necessary precursor before we can sell and distribute product to a client located in a foreign country. The OECD Member countries have not agreed to accept the BXA regulations and many of the countries in which our customers are doing business will not do so. Our proposal provides a palatable mechanism which could also be used by OECD members which could alter their position.

The Solution:

Clearly, there is no simple answer to the government's desire to protect US interests to thwart crime. Sophisticated tools are available everywhere, and it isn't necessary to use the escrowed key technology except for US provided systems. It is not illegal, difficult or expensive to employ security from international sources, so criminals can and will use them and thus avoid any eavesdroppers.

V-ONE is willing to assist in efforts to resolve these dilemmas, by participation in the NIST Inter- agency Working Group on Encryption and any other appropriate projects. Our inputs may not contribute a solution, but without understanding the feelings of our customers, the US efforts may continue to ignore the real problems with the key escrow system, resulting in regulations that squeeze V-ONE and other US producers of security technology out of the international market. Since this is a global marketplace, the result will even drive V-ONE and our US competitors out of the domestic market. International security vendors are successfully selling in the US because of their ability to satisfy global customers without concern for US export limitations.

Sincerely,

Charles B. Griffs,
Senior Vice President & Chief Financial Officer